Intelligent Spectrum Control in Heterogeneous Networks With High Security Capability

Chenxi Li*, Zan Li*†, *Senior Member, IEEE*, Jia Shi*, Lei Guan* and Lei Zhang‡

***Abstract*—In this letter, an intelligent spectrum control (ISC) scheme is proposed to enhance the communication security performance in heterogeneous networks (Het-Nets), where the available spectrum can be efficiently managed by avoiding interferences flexibly with the aid of spectrum sensing technique. We analyze the security performance for the Het-Nets, and derive the closed-form expressions for the reliable transmission probability and the secrecy probability of the authorized user. Our numerical simulation results validate the accuracy of the analytical expressions, and imply that the Het-Nets with the ISC scheme can achieve a high security performance.**

***Index Terms*—Intelligent spectrum control, communication security, reliable transmission probability, secrecy probability.**

I. Introduction

HETEROGENEOUS networks (Het-Nets), including a variety of different access networks to provide high-quality mobile services, have emerged to meet the needs of the next-generation communication for carrying an exponentially increasing amount of data traffic and massive number of terminals [1]. However, due to the openness of wireless channels and the broadcast nature of the radio propagation, the security of communication in Het-Nets has been widely concerned by various industries [2], such as the Internet of Things and the Cloud Computing. Moreover, as interferences become more complicated, preventing the private information from being intercepted by illegitimate users has further triggered public attention [3]. In addition, the diversity of access methods in Het-Nets also makes the means of interference or eavesdropping more flexible [4]. Therefore, it is essential to carry out theoretical researches on improving the communication security of Het-Nets.

Recently, some researches on the communication security of Het-Nets have been investigated in [5]–[8]. The authors in [5], [6] introduced friendly jammers to maximize the secrecy rate of data transmission from different perspectives. Besides, additional artificial noise (AN) has been injected towards eavesdroppers by full-duplex users in [6]. In addition, Wu *et al.* [7] deployed more low-power base stations in high path-loss environments to improve security performance. Furthermore, an artificial-noise-aided secure beamforming strategy has been designed in [8] to maximize the secrecy rate of the receiver.

Nevertheless, the malicious communication interference usually change randomly during the information transmission, which has rarely been studied by most existing methods for improving the security of Het-Nets. At the same time, since the tremendous popularity of smart devices has spurred the explosive growth of high-rate multimedia wireless services, existing methods of adding AN further increase the energy cost and signaling overhead.

In this letter, we propose an intelligent spectrum control (ISC) scheme, which can flexibly avoid malicious interferences with the aid of spectrum sensing, and does not require additional energy cost and signaling overhead for introducing AN. In addition, we analyze the security performance of the ISC scheme. In particular, the closed-form expressions for the reliable transmission probability and the secrecy probability of the authorized user are derived, so as to improve the security of Het-Nets by adjusting the parameters of the proposed scheme. Comprehensive simulation analyses are provided: 1) validating the accuracy for our analysis of the security performance of the Het-Nets; 2) revealing that the ISC scheme aided Het-Nets can achieve a higher security performance by comparing with existing security schemes, while obtaining reliable transmission probability without too much secrecy loss.

II. System Model

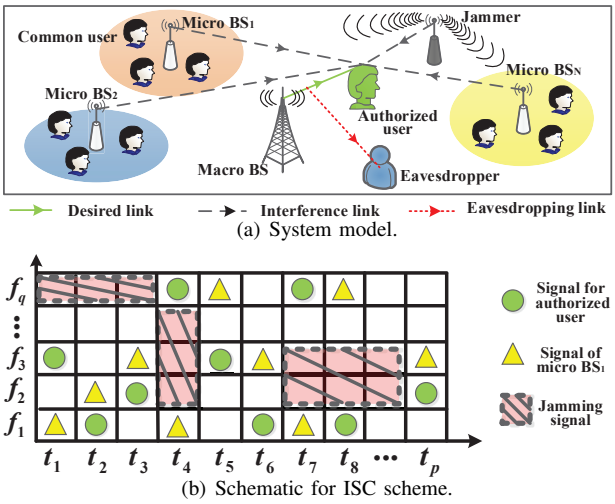

Fig. 1. System model and ISC scheme.

A. System Description and Assumptions

We consider a Het-Net as shown in Fig. 1(a), where a macro BS serving an authorized user is overlaid with multiple micro BS_m $(m = 1, 2, \cdots, N)$, each of which supports a cluster of common users [1], [6]. Without loss of generality, the macro BS located in the center of the network, and the micro BSs are distributed following Poisson point process (PPP). Assume that each link in the Het-Net experiences independent Rayleigh fading. Specifically, we focus on investigating the downlink transmission for the typical authorized user and the eavesdropper. As shown in Fig. 1(a), the security threats to the communication link between authorized users and the macro BS can be divided into three parts: (1) malicious interference, (2) inter-layer interference, (3) the existence of the eavesdropper.

*State Key Lab. ISN, Xidian University, Xi'an, China.
†Collaborative Innovation Center of Information Sensing and Understanding, Xi'an, China.
‡School of Engineering, University of Glasgow, Glasgow, G12 8QQ, UK.
This research was supported by NSFC 61825104, 61501354, 61501356, 61901328. (*Corresponding author*: *Zan Li* and *Lei Guan*: zanli@xidian.edu.cn)

Accordingly, the signal-to-interference-plus-noise ratio (SINR) of the authorized user and eavesdropper can be expressed as

$$\text{SINR}_u = \frac{P_u}{I_{ex,u} + I_{in,u} + N_0}, \text{SINR}_e = \frac{P_e}{I_{ex,e} + I_{in,e} + N_0}, \tag{1}$$

where P_u and P_e represent the received signal power of the authorized user and the eavesdropper, respectively. Moreover, $I_{ex,x}$ and $I_{in,x}$ ($x \in \{u, e\}$) are the external and inter-cell interference power. Furthermore, N_0 is the background noise, which is characterized by a zero-mean, complex Gaussian random variable. In our network, the frequency reuse factor is assumed to be one, which means all the spectrum can be used by each BS. Note that, time slots set is $T = \{t_i \,|i = 1, 2, \cdots, p\}$ and the frequency slots set can be denoted by $F = \{f_j \,|j = 1, 2, \cdots, q\}$.

B. ISC Scheme

To design a Het-Net with high security capability, we develop a efficient frequency hopping multiple access technique, namely ISC scheme, which motivates to improve the security capability. The proposed ISC scheme aims to develop a good sequence family by finding and removing the frequency slots occupied by interferences. The designed sequence family is able to map the available frequency slots to the authorized users for realizing secure communication. In particular, our proposed scheme can exploit the advantages of efficiently avoiding malicious interference and demanding low energy cost. The detailed principles of our ISC scheme is summarized in Algorithm 1.

Algorithm 1 Principles of ISC scheme

Input: Frequency slots set F.

1: Determine the status of the entire frequency slots $P = \{P_{\text{f}_1}, P_{\text{f}_2}, \cdots, P_{\text{f}_q}\}$, $P_{\text{f}_j} \in \{0, 1\}$. Note, if $P_{\text{f}_j} = 1$, f_j is occupied by interference, otherwise f_j is available. (By leveraging HOCs-based spectrum sensing method [9].)
2: Get the available frequency slots set F_A with q_A frequency slots after removing $F_I = \{f_j \,|P_{f_j} = 1\}$ from F.
3: **for** $t_i = \{t_1, t_2, \cdots, t_p\}$
4: Generate a sequence $Y = \{\mathbf{y}_{t_i}\}$ based on the block cryptography [4]. Upon applying $\mathbf{s}_{t_i} = (t_i + \mathbf{y}_{t_i} + \mathbf{s}_{t_{i-1}}) \bmod (q_A)$, the ISC sequence can be derived as $S_{t_i} = \{\mathbf{s}_{t_i}\}$ where $\mathbf{s}_{t_i} = \{\text{A}_{t_i,user}, \text{A}_{t_i,m_1}, \text{A}_{t_i,m_2}, \cdots, \text{A}_{t_i,m_N}\}$.
5: **end for**

Output: The ISC sequence family $\{S_{t_1}, S_{t_2}, \cdots, S_{t_p}\}$.

III. Performance Analysis

This section analyzes the security performance of the Het-Net in terms of the reliable transmission probability and the secrecy probability of the authorized user respectively.

A. Minimum Collision Probability

As introduced by [10], the collision probability has a direct impact on the probability that the transmitted signal will be correctly received by the receiver in our network.

Suppose that, the data transmission for each user requires L number of time slots, which happens independently and randomly. Once a demand occurs, the BS immediately starts transmitting information to the user. If there is a collision between users, they will retransmit after stepping back for a period of time. It should be pointed out that, the arrival rate of an initial transmission for a user and the arrival rate of a retransmission are subject to the Poisson distribution, which are denoted by μ and θ, respectively. Therefore, when combining the scenarios of initial transmission and re-transmission, the total arrival rate G for transmitting information to a user can be given by $G = \mu + \theta$. The probability of transferring n data in unit time can be expressed as $f(n) = (G^n \cdot e^{-G})/(n!)$.

Since each user can independently and randomly complete the signal transmission by using asynchronous multiple access, we first analyze the scenario that two users (i.e., user U_1 and user U_2) do not conflict during the data transmission. The transmission on the $l_1 \sim l_{m-1}$ time slot for user U_1 will overlap with that for user U_2 by at least two consecutive time slots. In a little more detail, the l_m time slot of user U_1 will overlap with the last time slot of user U_2. Accordingly, users U_1 and U_2 will have m ($m \leq p$) time slots overlapping during the transmission process. Therefore, in the Het-Nets considered, the probability that two users do not have frequency collision is

$$\Pr(l_i, q) = \Pr(f_{l_i}^1 \neq f_{l_i}^2, f_{l_{i+1}}^1 \neq f_{l_i}^2; i = 1, 2, \cdots, m). \tag{2}$$

Since the frequency slots chosen for a user are independent on different time slots, $\Pr(l_i, q)$ can be further denoted by

$$\Pr(l_i, q) = \prod_{l_i=1}^{m} \Pr(f_{l_i}^1 \neq f_{l_i}^2, f_{l_{i+1}}^1 \neq f_{l_i}^2). \tag{3}$$

Based on the conditional probability above, we can obtain

$$\begin{aligned} &\Pr(l_i, q(t)) \\ &= \prod_{l_i=1}^{m} \sum_{1}^{q(t)} \Pr(f_{l_i}^1 \neq f_{l_i}^2, f_{l_{i+1}}^1 \neq f_{l_i}^2 \,\big|f_{l_i}^2 = f_t\,) \cdot \Pr(f_{l_i}^2 = f_t). \end{aligned} \tag{4}$$

Assuming $\Pr(f_l^2 = f_t) = P_t$, $\Pr(l_i, q(t))$ becomes

$$\begin{aligned} \Pr(l_i, q(t)) &= \prod_{l_i=1}^{m-1} \sum_{t=1}^{q(t)} (1 - P_t)^2 P_t + \sum_{t=1}^{q(t)} (1 - P_t) P_t \\ &= (\sum_{t=1}^{q(t)} (1 - P_t)^2 P_t)^{l_i - 1} + \sum_{t=1}^{q(t)} (1 - P_t) P_t, \end{aligned} \tag{5}$$

where $\sum_{t=1}^{q(t)} P_t = 1$, and $0 \leq P_t \leq 1$.

In order to obtain the maximum value of $\Pr(l_i, q(t))$, we apply the derivation in [10] to (5). It readily knows that the maximum value of $Pr(l_i, q(t))$ can only be acquired when all frequency slots can be selected with equal probability. In this case, the maximum value of $Pr(l_i, q(t))$ can be written by

$$\Pr_{\max}(l_i, q(t)) = (1 - (1/q(t)))^{2l-1}. \tag{6}$$

Considering the randomness of the overlapped frequency slots $l_i \in \{1, 2, \cdots, L\}$, we have $\Pr(l_i) = 1/L$. Therefore, in the Het-Net conceived, for any given time, the probability that user U_1 and user U_2 do not collide is

$$\Pr(L, q(t)) = \sum_{l=1}^{L} \Pr_{\max}(l_i, q(t)) \Pr(l_i) = \sum_{l=1}^{L} (1 - \tfrac{1}{q(t)})^{2l-1} \tfrac{1}{L}. \tag{7}$$

Since the number of time slots L used for a signal is much smaller than the number of frequency slots available $q(t)$ in the actual communication system, we use Taylor's formula to further develop (7) and approximate the high-order infinitesimal term. Hence, we have

$$\Pr(L, q(t)) \approx \sum_{l=1}^{L} (1 - \frac{2l - 1}{q(t)}) \frac{1}{L} = 1 - L/q(t). \tag{8}$$

Accordingly, the minimum collision probability for user U_1 and user U_2 in the Het-Net considered can be given by

$$\Pr_c = 1 - \Pr(L, q(t)) = L/q(t). \tag{9}$$

B. Reliable Transmission Probability

The reliable transmission probability of the authorized user can be described by

$$P(\delta_u) = \Pr(\text{SINR}_{u,\text{BS}} \geq \delta_u), \tag{10}$$

which is the probability that the authorized user can decode the received signal, i.e., the SINR of the authorized user is greater than the SINR decoding threshold for the authorized user δ_u.

In the ISC scheme, let us denote the probability of the BS using an available frequency slot by $\Pr(f_T)$, where $f_T \in F_T$ and T is an arbitrary number from 1 to q. Then, the desired signal power and inter-user interference power received by the authorized user can be expressed as

$$\begin{aligned} P_u &= \frac{P_{\text{BS}}}{L} \sum_{l=1}^{L} \sum_{T=1}^{q} \Pr(f_T) \left|h_{u\cdot f_T \cdot l}\right|^2, \\ I_{in,u} &= \frac{P_{bs_i}}{L} \sum_{l=1}^{L} \sum_{T=1}^{q} \sum_{i=1}^{n} \Pr_c \Pr(i_1 \cdot f_T) \left|h_{f_T \cdot l}\right|^2, \end{aligned} \tag{11}$$

where P_{BS} and P_{bs} represent the total power transmit by the macro BS and the micro BS respectively, and L represents the time slots number of transmitted signal.

We assume $g_{u,\text{BS}} = \left|h_{u\cdot f_T}\right|^2$ is the channel gain between the macro BS and authorized user, which follows exponential distribution with parameter α, and $g_{(u,bs)} = \left|h_{i_1 \cdot f_T}\right|^2$ is the channel gain between micro BS_i and authorized user, which follows exponential distribution with parameter β_i.

Upon substituting (9) and (11) into (1), the SINR of the authorized user can be rewritten as

$$\text{SINR}_u = \frac{\frac{P_{\text{BS}}}{L} \sum\limits_{l=1}^{L} \sum\limits_{T=1}^{q} \Pr(f_T) \left|h_{u\cdot f_T \cdot l}\right|^2}{P_{bs_i} \sum\limits_{l=1}^{L} \sum\limits_{T=1}^{q} \sum\limits_{i=1}^{n} \frac{1}{\text{q}} \Pr(f_T) \left|h_{i_1 \cdot f_T \cdot l}\right|^2 + N_0}. \tag{12}$$

Based on (12), we can now derive the following theorem.

Theorem 1. *The reliable transmission probability for the authorized user can be given by*

$$P(\delta_u) = \left(\frac{(P_{BS}/L)\alpha^2}{(P_{BS}/L)\alpha^2 + P_{bs}\beta^2\delta_u/q}\right)^n \exp\left(-\frac{\delta_u N_0 L}{P_{BS}\alpha^2}\right). \tag{13}$$

Proof. Please refer to the Appendix. □

C. Secrecy Probability

The secrecy probability is defined as the probability that an eavesdropper can not receive the valid information, expressed as

$$P(\delta_e) = \Pr(\text{SINR}_{e,\text{BS}} \leq \delta_e). \tag{14}$$

Assume that the eavesdropper does not know the sequence S, which is also the common case for most practical systems. Therefore, the eavesdropper accesses a random frequency slot to intercept the transmitted signal, but also increases the chance of the eavesdropper colliding with all micro BSs and authorized users. Consequently, the total power of intercepted signals by the eavesdropper and the inter-user interference to the eavesdropper can be expressed as

$$P_e = \frac{P_{\text{BS}}}{L} \sum_{l=1}^{L} \left|h_{e\cdot f_T \cdot l}\right|^2, \; I_{in,e} = \frac{P_{bs_i}}{L} \sum_{l=1}^{L} \sum_{i=1}^{n-1} \Pr_c \left|h_{i_2 \cdot f_T \cdot l}\right|^2. \tag{15}$$

Furthermore, the channel gain $g_{(e,\text{BS})} = \left|h_{e\cdot f_T}\right|^2$ between the eavesdropper and the macro BS follows the exponential distribution of parameter λ. Similarly, the channel gain $g_{(e,bs)} = \left|h_{i_2\cdot f_T}\right|^2$ between the eavesdropper and a micro base station BS_i obeys the exponential distribution of parameter ω_i.

Substituting (9) and (15) into (1), the SINR of the eavesdropper can be rewritten as

$$\text{SINR}_e = \frac{\frac{P_{\text{BS}}}{L} \sum\limits_{l=1}^{L} \left|h_{e\cdot f_T \cdot l}\right|^2}{P_{bs_i} \sum\limits_{l=1}^{L} \sum\limits_{i=1}^{n-1} \frac{1}{q} \left|h_{e\cdot f_T \cdot l}\right|^2 + N_0}. \tag{16}$$

With (16), we can derive the following theorem.

Theorem 2. *The secrecy probability can be expressed as*

$$P(\delta_e) = 1 - \left(\frac{(P_{BS}/L)\lambda^2}{(P_{BS}/L)\lambda^2 + P_{bs}\omega^2\delta_e/q}\right)^{n-1} \exp\left(-\frac{\delta_e N_0 L}{P_{BS}\lambda^2}\right). \tag{17}$$

Proof. It is similar to that of Theorem 1, hence, is omitted due to the lack of space. □

IV. Numerical Results

This section presents the simulation results to evaluate the security performance of the Het-Nets. In our simulation, we assume, there are one macro BS, ten micro BSs, one jammer, one eavesdropper. Further, we set $\alpha = 5$, $\lambda = 3$, $\delta_u = \delta_e = 3$, $\beta_i = 2$ and $\omega_i = 1, \forall i \in \{1, 2, \cdots, 10\}$.

Figure 2 shows the variation of the reliable transmission probability and the secrecy probability with the signal to noise ratio (SNR) when q is equal to 128. From this figure, we can obtain the following observations. Firstly, the simulation results of reliable transmission probability and secrecy probability perfectly match the theoretical results, which verifies the correctness of the proposed scheme. Secondly, the reliable transmission probability increases exponentially with the increase of SNR, while the secrecy probability decreases approximatively linearly. This indicates that, as communication environment becomes better, the possibility of the authorized user receiving complete information increases rapidly, while the probability that eavesdropper receives effective information stays in a region of small values. Thirdly, by comparing with the method of adding artificial noise used in literature [6], which is one of the typical methods for improving the security of communication systems, the proposed ISC scheme can achieve higher security performance of Het-Nets (i.e., the SNR gain is 0.4 dB when the reliable transmission probability is 0.35 and the secrecy probability is 0.065). It is worth noting that compared with the method of adding artificial noise, the proposed ISC scheme does not need to occupy the transmission power, nor does it need to know the location of the receiver in advance, thus the complexity of realizing the scheme is effectively reduced. In addition, as the threshold δ_u and δ_e increases from 1 to 3, the reliable transmission probability decreases while the secrecy probability increases. This indicates that the better the channel conditions required for transmitting signal, the more vulnerable the entire Het-Nets is to the security threat.

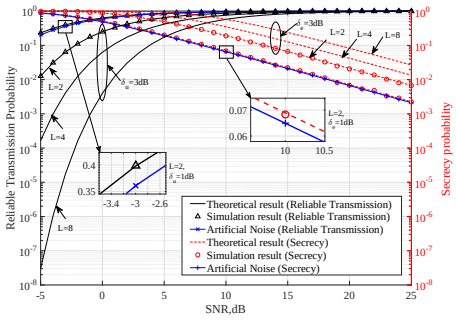

Fig. 2. The probability varies with the SNR under two sets of different SINR thresholds and $L = 2$, $4, 8$ when $q = 128$.

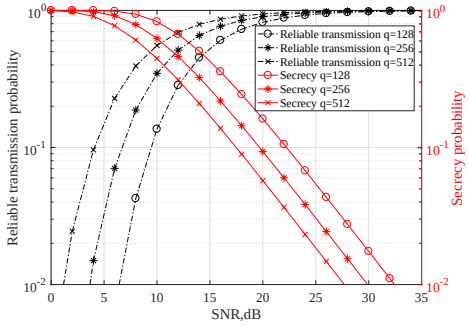

Fig. 3. The probability varies with the SNR under $q = 128, 256, 512$ when $\delta_u = \delta_e = 3$ and $L = 2$.

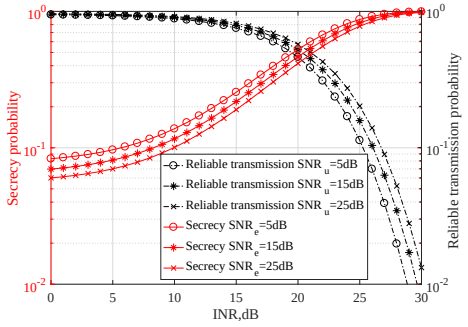

Fig. 4. The probability varies with the INR under SNR = 5dB, 15dB, 25dB when $\delta_u = \delta_e = 3$, $L = 2$ and $q = 128$.

Moreover, Fig. 2 and Fig. 3 show the relationship between reliable transmission probability and secrecy probability when varying L and q, respectively. It can be clearly seen that with the increase of L and the decrease of q, the reliable transmission probability decreases while the secrecy probability increases. This is because the use of more time slots or less frequency slots will increase the user collision probability and decrease the security of the entire Het-Nets. Hence, it is better to choose small L and large q to enhance the network security.

Figure 4 shows the reliable transmission probability and the secrecy probability against interference-to-noise ratio (INR) under different SNRs. When the SNR is fixed, the reliable transmission probability decreases as the INR increases, while the secrecy probability increases. Since the power of the jamming signal is increased, the transmission of the signal is blocked. In that case, it becomes more difficult for the authorized user to receive the complete information, and the network becomes less secure.

V. Conclusion

In this paper, we have proposed the ISC scheme in a Het-Net for achieving high security capability. By leveraging spectrum sensing technique, our proposed scheme flexibly avoid malicious interferences with the aid of spectrum sensing. Furthermore, we have analyzed the security performance of the ISC scheme assisted Het-Nets. Specifically, the closed-form expressions for the reliable transmission probability and the secrecy probability of the authorized user have been derived. Simulation results have validated the accuracy of the theoretical expressions for the security performance, and have revealed that the proposed ISC scheme can be a promising candidate for future Het-Nets to achieve high security performance.

Appendix

To simplify the calculation, we denote that

$$X=\sum_{l=1}^{L}\sum_{T=1}^{q}\Pr(f_T)|h_{u\cdot l}|^2, Y=\sum_{i=1}^{\mathrm{n}}P_{bs_i}\sum_{l=1}^{L}\sum_{T=1}^{q}\Pr(f_T)|h_{i_1\cdot l}|^2. \tag{18}$$

Since $|h_{u\cdot l}|^2 \sim E(\alpha)$ and $|h_{i_1\cdot l}|^2 \sim E(\beta_i)$, the probability density function (PDF) of X and Y can be obtained, as follows:

$$f_X(x) = \frac{1}{\alpha^2}e^{-\frac{1}{\alpha^2}}, f_Y(y) = \frac{y^{n-1}}{\Gamma(n)(P_{bs_i}\beta_i^2)^n}\exp(-\frac{y}{P_{bs_i}\beta_i^2}). \tag{19}$$

When assuming $P_{bs_i} = P_{bs}$ $(i = 1, 2, \cdots, n)$, the reliable transmission probability for the authorized user becomes

$$\begin{aligned}
P(\delta_{\mathrm{u}}) &= \Pr(\mathrm{SINR_u} \geq \delta_u) \\
&= \Pr\left(\frac{1}{(1/q)Y + N_0}\min((P_{\mathrm{BS}}/L)X) \geq \delta_u\right) \\
&= \int_0^{\infty}\int_{\frac{\delta_{\mathrm{u}}((1/q)y+N_0)L}{P_{\mathrm{BS}}}}^{\infty} f_X(x)f_Y(y)dxdy \\
&= \int_0^{\infty}\exp\left(-\frac{\delta_u((1/q)y+N_0)L}{P_{\mathrm{BS}}\alpha^2}\right)f_Y(y)dy \\
&= \frac{\exp(-\frac{\delta_u N_0 L}{P_{\mathrm{BS}}\alpha^2})}{\Gamma(n)(P_{bs}\beta^2)^n}\int_0^{\infty} y^{n-1}\exp\left(-(\frac{\delta_u\cdot(L/q)}{P_{\mathrm{BS}}\alpha^2}) + \frac{y}{P_{bs}\beta^2}\right)dy \\
&= \left(\frac{(P_{\mathrm{BS}}/L)\alpha^2}{(P_{\mathrm{BS}}/L)\alpha^2 + P_{bs}\beta^2\delta_u/q}\right)^n \exp(-\frac{\delta_u N_0 L}{P_{\mathrm{BS}}\alpha^2}).
\end{aligned} \tag{20}$$

References

[1] M. G. Kibria, G. P. Villardi, K. Nguyen, *et al.*, "Heterogeneous networks in shared spectrum access communications," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 1, pp. 145-158, Jan. 2017.

[2] L. Zhang, G. Ding, Q. Wu, *et al.*, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342-1363, Apr. 2015.

[3] Y. Zou, J. Zhu, X. Wang, *et al.*, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, Sept. 2016.

[4] Z. Li, L. Guan, C. Li, *et al.*, "A secure intelligent spectrum control strategy for future THz mobile heterogeneous networks," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 116-123, June 2018.

[5] I. Bang, S. M. Kim, and D. K. Sung, "Opportunistic user selection with adaptive jamming for secure communication in heterogeneous networks," in *Proc. IEEE PIMRC*, 2014, pp. 42-46.

[6] W. Tang, S. Feng, Y. Ding, *et al.*, "Physical layer security in heterogeneous networks with jammer selection and full-duplex users," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 7982-7995, Sept. 2017.

[7] H. Wu, X. Tao, N. Li, *et al.*, "Secrecy outage probability in multi-rat heterogeneous networks," *IEEE Commun. Lett.*, vol. 20, no. 1, pp. 53-56, Jan. 2016.

[8] B. Li, Z. Fei, Z. Chu, *et al.*, "Secure transmission for heterogeneous cellular networks with wireless information and power transfer," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3755-3766, Dec. 2018.

[9] D. Wang, N. Zhang, Z. Li, *et al.*, "Leveraging high order cumulants for spectrum sensing and power recognition in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 1298-1310, Feb. 2018.

[10] L. Guan, Z. Li, J. Si, *et al.*, "Analysis of asynchronous frequency hopping multiple-access network performance based on the frequency hopping sequences," *IET Commun.*, vol. 9, no. 1, pp. 117-121, Jan. 2015.